

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

Case No. 2:21-mj-395

information associated with GOOGLE ACCOUNT)
 WHEELERA66@GMAIL.COM at is stored at the)
 premises controlled by GOOGLE)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached hereto and incorporated herein by reference

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841	Possession with Intent to Distribute MDMA / LSD

The application is based on these facts:

See attached Affidavit

- ☐ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

Christopher D. Caplin, DEA Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/4/2021

City and state: Columbus, OH



Chelsey M. Vascara
 United States Magistrate Judge

Judge's signature

Chelsey M. Vascara, United States Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH THE
GOOGLE ACCOUNT
WHEELERA66@GMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE LLC

Case No. 2:21-mj-395

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, United States Drug Enforcement Administration (DEA) Special Agent Christopher D. Caplin being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC (hereafter “Google”) to disclose to the government records and other information, including the contents of communications, associated with the above-listed Google Account that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheater Parkway, Mountain View, CA 94043. The information to be disclosed by Google and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the United States Drug Enforcement Administration (DEA) and have been employed since March 2008. I am assigned to the Detroit Field Division, Columbus District Office. As such, I am an “investigative or law enforcement officer” of the United States within the meaning of Title 18 U.S.C. § 2510(7), that is, an officer of the United States empowered by law to conduct criminal investigations and make arrests for offenses

enumerated in 18 U.S.C. § 2516. Your affiant is empowered to investigate, to make arrests with or without warrants, and to execute search warrants under the authority of 21 U.S.C. § 878. Prior to being employed by the DEA, your affiant was employed by the Indianapolis Metropolitan Police Department located in Indianapolis, Indiana, from September 2000 to March 2008.

During this time, your affiant has accumulated the following training and experience:

Completed the DEA Basic Agent Training Academy in Quantico, VA where I received specialized narcotics-related training includes drug identification, interview and interrogation, managing informants, undercover operations, conspiracy investigations, surveillance and electronic monitoring techniques, tactical application of narcotics enforcement, search and seizure law, pharmaceutical diversion, clandestine drug labs, marijuana cultivation and money laundering investigations. During my law enforcement career, your Affiant has participated in and conducted numerous investigations of violations of various State and Federal criminal laws, including the unlawful possession with intent to distribute controlled substances, the distribution of controlled substances and conspiracy to possess with the intent to distribute controlled substances, in violation of Title 21, United States Code. These investigations have resulted in seizures of illegal drugs and drug proceeds, as well as the arrests of individuals who have distributed marijuana, cocaine, heroin, and methamphetamine, as well as other controlled substances.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence, contraband, instrumentalities, and/or fruits of violations of 21 U.S.C. § 841, as described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. In early December, 2019, investigators from the Central Ohio Cyber Drug Task Force (COCDTF) identified a dark web drug vendor operating under the moniker “INSTRUMENT.” Information gathered from the dark web indicated that “INSTRUMENT” was active on several marketplaces advertising sales of various controlled substances that would be shipped to and from the United States. Investigators learned that in July of 2019, a drug task force in Sacramento, California, made an undercover (UC) purchase over the dark web from “INSTRUMENT” of approximately one gram of methylenedioxy-methamphetamine (MDMA).

7. Between December 2019 and May 2020, COCDTF investigators in Columbus, Ohio, made four UC purchases off the dark web marketplace “Empire” from “INSTRUMENT.” The purchases included 25 dosage units of lysergic acid diethylamide (LSD) on December 12, 2019; five grams of MDMA on December 22, 2019; five dosage units of LSD on April 23, 2020; and five grams of MDMA on May 4, 2020. Each order took approximately one week to arrive in Columbus, and were sent via United States Postal Service (USPS) from different return addresses in the Minneapolis/St. Paul, Minnesota area.

8. In February of 2021, while conducting blockchain analysis on seized market place data associated with "INSTRUMENT," COCDTF investigators identified 127 transactions originating in INSTRUMENT's dark web vendor wallets that were sent to BitPay.com.

9. On February 26, 2021, COCDTF investigators sent a subpoena to Subpoenas@BitPay.com requesting all information associated with the transactions. On March 11, 2021, BitPay responded with a spreadsheet identifying 129 transactions, consisting of a total of 95.371032 bitcoin valued at approximately \$43,400.11 at the time of the transactions. The spreadsheet identified the following transactions:

- Five transactions between March 9, 2014 through April 18, 2014 for approximately \$6,693.96 sent to BtcTrip, a website that is no longer in existence, but a clear web search indicates it was a website designed to allow users to buy plane tickets using bitcoin.
- 105 transactions between February 24, 2014 through March 28, 2015 for approximately \$24,592.62 sent to Gyft Inc., a website that allows you to buy, send, and redeem gift cards for over 200 different retailers.
- One transaction on December 07, 2014 for approximately \$35.01 sent to Namecheap.com, a website that allows users to buy internet domains (website addresses).
- 17 transactions between April 29, 2014 through June 17, 2014 for approximately \$12,067.56 sent to SnapCard, which allowed users to pay with bitcoin at online retailers that don't officially accept cryptocurrency. The company has since been purchased by Wyre, a payment service.

- One transaction on July 8, 2014 for approximately \$10.96 sent to Warner Bros. Records.

The transaction had a buyer's email address listed as Chris.Volden@gmail.com.

10. On March 15, 2021, investigators sent a subpoena to LegalPapers@Fiserv.com regarding any information on the 105 transactions conducted on Bitpay.com to Gyft, Inc. On April 6, 2021 Fiserv responded with a spreadsheet identifying 165 transactions, worth approximately \$33,113.37, belonging to the same user account, identified by Gyft ID 76900276-6043-4ce8-89b0-d9211aa90090. The account listed three email addresses, Chris.Volden@gmail.com, Chris@bellslabradors.com, and Zaneisgreat@lelantos.org. All gift cards purchased were marked "self-gifted" and for big box retailers, restaurants and entertainment services. Investigators know it is common for Darknet Vendors to cash out their bitcoin in the form Gift Cards to avoid detection and report requirements from banks and law enforcement. Gyft, Inc. also listed the IP Addresses used during each transaction. A search of the IP address locations shows the transactions were conducted in, Saint Paul, Minnesota; Chicago, Illinois; Volin, South Dakota; and New York, New York; with the majority being conducted in Saint Paul, Minnesota.

11. A law enforcement database search of the email address Chris.Volden@gmail.com identified the user as Christopher Bryan VOLDEN with a date of birth of July 1, 1985. A public records check of VOLDEN listed his address as 4733 Bouleau Road, White Bear Lake, Minnesota, a suburb of Saint Paul. The prior UC drug buys from INSTRUMENT revealed all the packages were shipped from the Minneapolis/Saint Paul, Minnesota area.

12. Investigators also learned from Homeland Security Investigations (HSI) New York that VOLDEN was being investigated in 2013 for selling bitcoin to a known dark web

market vendor on the marketplace “Silk Road.” At the time, HSI New York identified VOLDEN's moniker as POLYGAMUS and POLYGAMUZ. A U.S. Customs and Border Protection Database query revealed VOLDEN was the subject of three seizures, including 17.5 grams of LSD in 2016, 3.3 grams of cocaine in 2013, and 107 grams of MDMA in 2013.

13. Investigators also learned that on February 19, 2013, VOLDEN was arrested by Saint Paul Police Department (SPPD) for selling synthetic narcotics. VOLDEN admitted to SPPD that he and his girlfriend, Angela WHEELER, sold numerous controlled substance over the internet, specifically on “Silk Road” marketplace. VOLDEN explained that he had started the business and made the initial orders of their products, and WHEELER often helped him by sending/receiving orders of controlled substances through the mail. A check of VOLDEN's criminal history confirmed the SPPD arrest, but not a conviction. Investigators believe VOLDEN or WHEELER switched the dark web moniker from POLYGAMUS to INSTRUMENT after the arrest.

14. On May 6, 2021, COCDTF investigators sought and received authorization for a federal search warrant on the Google account Chris.Volden@gmail.com. On May 11, 2021, Google provided the requested information associated with that account. While analyzing the records from Google, COCDTF investigators identified various other email addresses in contact with VOLDEN, including Wheeler66@gmail.com. In VOLDEN's account, Wheeler66@gmail.com is attributed to Angela WHEELER, his known girlfriend. Also, in a Google chat that took place on March 28, 2021, the user of Wheeler66@gmail.com identified themselves as Angela Wheeler.

15. Later in May 2021, COCDTF investigators made two additional UC purchases off the dark web marketplace “White House Market” from “INSTRUMENT.” The purchases

included 10 dosage units of LSD on May 11, 2021; and 50 dosage units of LSD on May 20, 2021. Following the May 11 purchase, investigators on surveillance followed VOLDEN to a United States Postal Service (USPS) drop box, and recovered an envelope with the same shipping address in Columbus that was used during the UC transaction. The envelope was photographed, repackaged, and forwarded to COCDTF investigators in Columbus. Following the May 20 purchase, investigators on surveillance saw VOLDEN and WHEELER leave their home together in the late afternoon, but did not see them stop at a USPS drop box and were unable to retrieve an envelope. COCDTF investigators, however, received the order in Columbus on May 26, 2021, that was post marked in Saint Paul, Minnesota, by USPS on May 20, 2021. USPS investigators advised COCDTF investigators that the letter would have had to have been mailed before 6:00 PM CST on May 20 in order to be post marked on May 20. COCDTF investigators believe VOLDEN and WHEELER dropped the order in a mailbox when they were together and out of view of investigators on surveillance.

16. Law enforcement sources in Minnesota confirmed for investigators that neither VOLDEN nor WHEELER have any known employment history for the last five years. However, in the search warrant information for VOLDEN's Google account, there were documents indicating VOLDEN paid approximately \$578,000 in March 2021 for the home he shares with WHEELER.

17. From your Affiant's training and experience, dark web users may store seed phrases, passwords, tracking numbers and/or ledgers on cell phones or their cloud-based storage. It is also law enforcement knowledge that dark web vendors will utilize email or various messenger apps to conduct business off the marketplace with trusted customers to avoid commission fees.

BACKGROUND CONCERNING GOOGLE¹

18. Google is a United States Company that offers to the public through its Google Accounts a variety of online services, including email, cloud storage, digital payments, and productivity applications, which can be accessed through a web browser or mobile applications. Google also offers to anyone, whether or not they have a Google Account, a free web browser called Google Chrome, a free search engine called Google Search, a free video streaming site called YouTube, a free mapping service called Google Maps, and a free traffic tracking service called Waze. Many of these free services offer additional functionality if the user signs into their Google Account.

19. In addition, Google offers an operating system (“OS”) for mobile devices, including cellular phones, known as Android. Google also sells devices, including laptops, mobile phones, tablets, smart speakers, security cameras, and wireless routers. Users of Android and Google devices are prompted to connect their device to a Google Account when they first turn on the device and a Google Account is required for certain functionalities on these devices.

20. Signing up for a Google Account automatically generates an email address at the domain gmail.com. That email address will be the log-in username for access to the Google Account. Enterprises may also establish Google Accounts which can be accessed using an email address at the enterprise’s domain (e.g. employee[@]company.com).

21. Google advertises its services as “One Account. All of Google working for you.” Once logged into a Google Account, a user can connect to Google’s full suite of services offered

¹ The information in this section is based on information published by Google on its public websites, including, but not limited to, the following webpages: the “Google legal policy and products” page available to registered law enforcement at lers.google.com; product pages on support.google.com; or product pages on about.google.com.

to the general public, described in further detail below. In addition, Google keeps certain records indicating ownership and usage of the Google Account across services, described further after the description of services below.

22. Google Drive is a cloud storage service automatically created for each Google Account. Users can store an unlimited number of documents created by Google productivity applications like Google Docs (Google's word processor), Google Sheets (Google's spreadsheet program), Google Forms (Google's web form service), and Google Slides, (Google's presentation program). Users can also upload files to Google Drive, including photos, videos, PDFs, and text documents, until they hit the storage limit. Users can set up their personal computer or mobile phone to automatically back up files to their Google Drive Account. Each user gets 15 gigabytes of space for free on servers controlled by Google and may purchase more through a subscription plan called Google One. In addition, Google Drive allows users to share their stored files and documents with up to 100 people and grant those with access the ability to edit or comment. Google maintains a record of who made changes when to documents edited in Google productivity applications. Documents shared with a user are saved in their Google Drive in a folder called "Shared with me." Google preserves files stored in Google Drive indefinitely, unless the user deletes them.

23. Google Keep is a cloud-based notetaking service that lets users take notes and share them with other Google users to view, edit, or comment. Google Keep notes are stored indefinitely, unless the user deletes them. Android device users can also use Google Drive to backup certain data from their device. Android backups on Google Drive may include mobile application data, device settings, file downloads, and SMS messages. If a user subscribes to

Google's cloud storage service, Google One, they can opt to back up all the data from their device to Google Drive.

24. Google provides email services (called Gmail) to Google Accounts through email addresses at gmail.com or enterprise email addresses hosted by Google. Gmail can be accessed through a web browser or a mobile application. Additional email addresses ("recovery," "secondary," "forwarding," or "alternate" email addresses) can be associated with the Google Account by the user. Google preserves emails associated with a Google Account indefinitely, unless the user deletes them.

25. Google provides an address book for Google Accounts through Google Contacts. Google Contacts stores contacts the user affirmatively adds to the address book, as well as contacts the user has interacted with in Google products. Google Contacts can store up to 25,000 contacts. Users can send messages to more than one contact at a time by manually creating a group within Google Contacts or communicate with an email distribution list called a Google Group. Users have the option to sync their Android mobile phone or device address book with their account, so it is stored in Google Contacts. Google preserves contacts indefinitely, unless the user deletes them. Contacts can be accessed from the same browser window as other Google products like Gmail and Calendar.

26. Google provides an appointment book for Google Accounts through Google Calendar, which can be accessed through a browser or mobile application. Users can create events or RSVP to events created by others in Google Calendar. Google Calendar can be set to generate reminder emails or alarms about events or tasks, repeat events at specified intervals, track RSVPs, and auto-schedule appointments to complete periodic goals (like running three times a week). A single Google Account can set up multiple calendars. An entire calendar can be

shared with other Google Accounts by the user or made public so anyone can access it. Users have the option to sync their mobile phone or device calendar, so it is stored in Google Calendar. Google preserves appointments indefinitely, unless the user deletes them. Calendar can be accessed from the same browser window as other Google products like Gmail and Calendar.

27. Google provides several messaging services including Duo, Messages, Hangouts, Meet, and Chat. These services enable real-time text, voice, and/or video communications through browsers and mobile applications, and also allow users to send and receive text messages, videos, photos, locations, links, and contacts. Google may retain a user's messages if the user hasn't disabled that feature or deleted the messages, though other factors may also impact retention. Google does not retain Duo voice calls, though it may retain video or voicemail messages.

28. Google offers a cloud-based photo and video storage service called Google Photos. Users can share or receive photos and videos with others. Google Photos can be trained to recognize individuals, places, and objects in photos and videos and automatically tag them for easy retrieval via a search bar. Users have the option to sync their mobile phone or device photos to Google Photos. Google preserves files stored in Google Photos indefinitely, unless the user deletes them.

29. Google offers a map service called Google Maps which can be searched for addresses or points of interest. Google Maps can provide users with turn-by-turn directions from one location to another using a range of transportation options (driving, biking, walking, etc.) and real-time traffic updates. Users can share their real-time location with others through Google Maps by using the Location Sharing feature. And users can find and plan an itinerary using Google Trips. A Google Account is not required to use Google Maps, but if users log into their

Google Account while using Google Maps, they can save locations to their account, keep a history of their Google Maps searches, and create personalized maps using Google My Maps. Google stores Maps data indefinitely, unless the user deletes it.

30. Google collects and retains data about the location at which Google Account services are accessed from any mobile device, as well as the periodic location of Android devices while they are in use. This location data can derive from a range of sources, including GPS data, Wi-Fi access points, cell-site locations, geolocation of IP addresses, sensor data, user searches, and Bluetooth beacons within range of the device. According to Google, this location data may be associated with the Google Account signed-in or registered to the device when Location Services are activated on the device and the user has enabled certain global settings for their Google Account, such as Location History or Web & App Activity tracking. The data retained may be both precision location data, like latitude and longitude coordinates derived from GPS, and inferential location data, such as the inference that a Google Account is in New York because it conducts a series of searches about places to eat in New York and directions from one New York location to another. Precision location data is typically stored by Google in an account's Location History and is assigned a latitude-longitude coordinate with a meter radius margin of error. Inferential data is stored with an account's Web & App Activity. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes it or opts to automatically delete their Location History and Web & App Activity after three or eighteen months. Accounts created after June 2020 auto-delete Location History after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

31. A subsidiary of Google, Google Payment Corporation, provides Google Accounts an online payment service called Google Pay (previously Google Wallet), which stores credit cards, bank accounts, and gift cards for users and allows them to send or receive payments for both online and brick-and-mortar purchases, including any purchases of Google services. Users may delete some data associated with Google Pay transactions from their profile, but Google Payment Corporation retains some records for regulatory purposes.

32. Google offers a free web browser service called Google Chrome which facilitates access to the Internet. Chrome retains a record of a user's browsing history and allows users to save favorite sites as bookmarks for easy access. If a user is logged into their Google Account on Chrome and has the appropriate settings enabled, their browsing history, bookmarks, and other browser settings may be saved to their Google Account in a record called My Activity.

33. My Activity also collects and retains data about searches that users conduct within their own Google Account or using the Google Search service while logged into their Google Account, including voice queries made to the Google artificial intelligence-powered virtual assistant Google Assistant or commands made to Google Home products. Google also has the capacity to track the websites visited using its Google Chrome web browser service, applications used by Android users, ads clicked, and the use of Google applications by iPhone users. According to Google, this search, browsing, and application use history may be associated with a Google Account when the user is logged into their Google Account on the browser or device and certain global settings are enabled, such as Web & App Activity. Google Assistant and Google Home voice queries and commands may also be associated with the account if certain global settings are enabled, such as Voice & Audio Activity tracking. Google maintains these records indefinitely for accounts created before June 2020, unless the user deletes them or opts in to

automatic deletion of their location history every three or eighteen months. Accounts created after June 2020 auto-delete Web & App Activity after eighteen months unless the user affirmatively changes the retention setting to indefinite retention or auto-deletion at three months.

34. Google Accounts can buy electronic media, like books, movies, and music, and mobile applications from the Google Play Store. Google Play records can include records of whether a particular application has been or is currently installed on a device. Users cannot delete records of Google Play transactions without deleting their entire Google Account.

35. Google offers a service called Google Voice through which a Google Account can be assigned a telephone number that can be used to make, record, and forward phone calls and send, receive, store, and forward SMS and MMS messages from a web browser, mobile phone, or landline. Google Voice also includes a voicemail service. Records are stored indefinitely, unless the user deletes them.

36. Google also offers a video platform called YouTube that offers Google Accounts the ability to upload videos and share them with others. Users can create a YouTube channel where they can upload videos, leave comments, and create playlists available to the public. Users can subscribe to the YouTube channels of others, search for videos, save favorite videos, like videos, share videos with others, and save videos to watch later. More than one user can share control of a YouTube channel. YouTube may keep track of a user's searches, likes, comments, and change history to posted videos. YouTube also may keep limited records of the IP addresses used to access particular videos posted on the service. Users can also opt into a setting to track their YouTube Watch History. For accounts created before June 2020, YouTube Watch History is stored indefinitely, unless the user manually deletes it or sets it to auto-delete after three or

eighteen months. For accounts created after June 2020, YouTube Watch History is stored for three years, unless the user manually deletes it or sets it to auto-delete after three or eighteen months.

37. Google integrates its various services to make it easier for Google Accounts to access the full Google suite of services. Users accessing their Google Account through their browser can toggle between Google Services via a toolbar displayed on the top of most Google service pages, including Gmail and Drive. Google Hangout, Meet, and Chat conversations pop up within the same browser window as Gmail. Attachments in Gmail are displayed with a button that allows the user to save the attachment directly to Google Drive. If someone shares a document with a Google Account user in Google Docs, the contact information for that individual will be saved in the user's Google Contacts. Google Voice voicemail transcripts and missed call notifications can be sent to a user's Gmail account. And if a user logs into their Google Account on the Chrome browser, their subsequent Chrome browser and Google Search activity is associated with that Google Account, depending on user settings.

38. When individuals register with Google for a Google Account, Google asks users to provide certain personal identifying information, including the user's full name, telephone number, birthday, and gender. If a user is paying for services, the user must also provide a physical address and means and source of payment.

39. Google typically retains and can provide certain transactional information about the creation and use of each account on its system. Google captures the date on which the account was created, the length of service, log-in times and durations, the types of services utilized by the Google Account, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account

via Google's website or using a mobile application), details about the devices used to access the account, and other log files that reflect usage of the account. In addition, Google keeps records of the Internet Protocol ("IP") addresses used to register the account and accept Google's terms of service, as well as the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the Google Account.

40. Google maintains the communications, files, and associated records for each service used by a Google Account on servers under its control. Even after a user deletes a communication or file from their Google Account, it may continue to be available on Google's servers for a certain period of time.

41. In my training and experience, evidence of who was using a Google Account, and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, where, when, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. This can be true even if subscribers insert false information to conceal their identity; this information often nevertheless provides clues to their identity, location or illicit activities.

42. For example, the stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. Based on my training and experience, messages, emails, voicemails, photos, videos, documents, and internet searches are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

43. In addition, the user's account activity, logs, stored electronic communications, location history, and other data retained by Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

44. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

45. Other information connected to a Google Account may lead to the discovery of additional evidence. For example, the identification of apps such as Wickr, Telegram and Tor downloaded from the Google Play Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

46. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

47. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

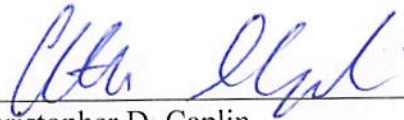
48. Based on the forgoing, I request that the Court issue the proposed search warrant.

49. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING


50. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Christopher D. Caplin
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me on June 4, 2021



HON. CHELSEY M. VASCURA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

1. This warrant applies to information associated with WHEELERA66@GMAIL.COM (the “account”) that is stored at premises owned, maintained, controlled, or operated by Google LLC [and/or Google Payment Corporation], a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

Attachment B

Particular Things to Be Seized

I. Information to be disclosed by Google LLC and/or Google Payment Corporation (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any information that has been deleted but is still available to the provider or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government for each account or identifier listed in Attachment A the following information since account creation, unless otherwise indicated:

Google Account

- a. All business records and subscriber information, in any form kept, pertaining to the account, including:
 - a. Names (including subscriber names, usernames, and screen names);
 - b. Addresses (including mailing addresses, residential addresses, business addresses, and email addresses, including alternate and recovery email addresses);
 - c. telephone numbers, including SMS recovery and alternate sign-in numbers;
 - d. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions, including log-in IP addresses;
 - e. Telephone or instrument numbers or other subscriber numbers or identities, including any temporarily assigned network address, SMS recovery numbers, Google Voice numbers, and alternate sign-in numbers
 - f. Length of service (including start date and creation IP) and types of service utilized;
 - g. Means and source of payment (including any credit card or bank account number);
 - h. Change history.
- b. All device information associated with the accounts, including but not limited to, manufacture names, model numbers, serial number, media access control (MAC) addresses, international mobile equipment identifier (IMEI) numbers, FCC ID numbers, Android IDs, and telephone numbers;
- c. Records of user activity for each connection made to or from the Account(s), including, for all Google services, the date, time, length, and method of connection, data transfer volume, user names, source and destination IP address, name of accessed Google service, and all activity logs

- d. The contents of all records associated with the account in Google Drive (including Docs, Sheets, Forms, and Slides) and Google Keep, including:
 - a. Files, folders, media, notes and note titles, lists, applications, and other data uploaded, created, stored, or shared with the account including drafts and deleted records
 - b. Third-party application data and backups
 - c. SMS data and device backups; the creation and change history of each record; accounts with access to or which previously accessed each record
 - d. Any location, device, other Google service (such as Google Classroom or Google Group), or third-party application associated with each record
 - e. All associated logs, including access logs and IP addresses, of each record.
- e. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, and deleted emails; attachments; the source and destination addresses associated with each email; the size, length, and timestamp of each email; and true and accurate header information including the actual IP addresses of the sender and recipients of the emails. All forwarding or fetching accounts relating to the accounts
- f. Any records pertaining to the user's contacts, including address books; contact lists; social network links; groups, including Google Groups to which the user belongs or communicates with; user settings; and all associated logs and change history.
- g. Any records pertaining to the user's calendar(s), including: Google Calendar events; Google Tasks; reminders; appointments; invites; and goals; the sender and recipients of any event invitation, reminder, appointment, or task; user settings; and all associated logs and change history
- h. The contents of all text, audio, and video messages associated with the account, including Chat, Duo, Hangouts, Meet, and Messages (including SMS, MMS, and RCS), in any format and however initially transmitted, including, but not limited to: stored, deleted, and draft messages, including attachments and links; the source and destination addresses associated with each communication, including IP addresses; the size, length, and timestamp of each communication; user settings; and all associated logs, including access logs and change history.
- i. The contents of all media associated with the account in Google Photos, including: photos, GIFs, videos, animations, collages, icons, or other data uploaded, created, stored, or shared with the account, including drafts and deleted records; accounts with access to or which previously accessed each record; any location, device, or third-party application data associated with each record; and all associated logs of each record, including the creation and change history, access logs, and IP addresses.
- j. All maps data associated with the account, including Google Maps and Google Trips, including: all saved, starred, and privately labeled locations; search history; routes begun;

routes completed; mode of transit used for directions; My Maps data; accounts and identifiers receiving or sending Location Sharing information to the account; changes and edits to public places; and all associated logs, including IP addresses, location data, and timestamps, and change history.

- k. All Location History and Web & App Activity indicating the location at which the account was active, including the source of the data, date and time, latitude and longitude, estimated accuracy, device and platform, inferences drawn from sensor data (such as whether a user was at rest, walking, biking, or in a car), and associated logs and user settings, including Timeline access logs and change and deletion history.
- l. All payment and transaction data associated with the account, such as Google Pay and Google Wallet, including: records of purchases, money transfers, and all other transactions; address books; stored credit; gift and loyalty cards; associated payment cards, including any credit card or bank account number, PIN, associated bank, and other numbers; and all associated access and transaction logs, including IP address, time stamp, location data, and change history
- m. All Internet search and browsing history, and application usage history, including Web & App Activity, Voice & Audio History, Google Assistant, and Google Home, including: search queries and clicks, including transcribed or recorded voice queries and Google Assistant responses; browsing history, including application usage; bookmarks; passwords; autofill information; alerts, subscriptions, and other automated searches, including associated notifications and creation dates; user settings; and all associated logs and change history.
- n. All activity relating to Google Play, including: downloaded, installed, purchased, used, and deleted applications, details of the associated device and Android ID for each application, medium, or file; payment transactions; user settings; and all associated logs, including IP addresses, timestamps, and change history.
- o. All Google Voice records associated with the account, including: forwarding and other associated telephone numbers, connection records; call detail records; SMS and MMS messages, including draft and deleted messages; voicemails, including deleted voicemails; user settings; and all associated logs, including access logs, IP addresses, location data, timestamps, and change history.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 21 U.S.C. § 841, those violations involving Angela Sue WHEELER including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Evidence of communications between co-conspirators and/or Darknet buyers.
Passwords, seed phrases or account information belonging to Darknet moniker “INSTRUMENT.” Financial transactions related to the distribution of narcotics on the Darknet.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner’s state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the user ID about matters relating to the sales of narcotics, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [PROVIDER], and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [PROVIDER]. The attached records consist of _____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of [PROVIDER], and they were made by [PROVIDER] as a regular practice; and

b. such records were generated by [PROVIDER'S] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of [PROVIDER] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by **[PROVIDER]**, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature